



フィッシングメールに注意！！



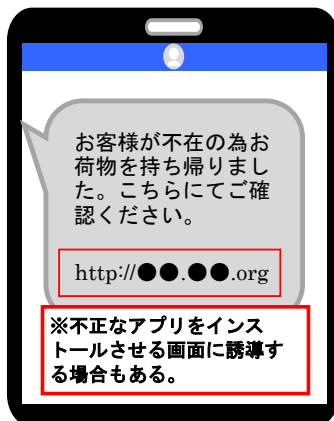
あなたの個人情報を狙う「フィッシングメール」の手口

フィッシング妖怪カッパル

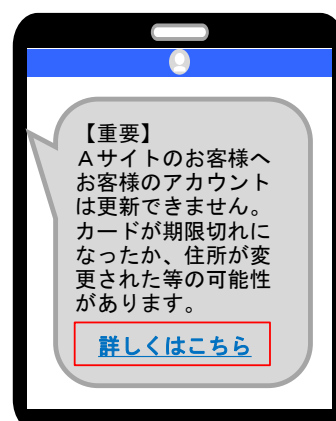
金融機関



宅配事業者



大手ショッピングサイト



クレジットカード会社



フィッシングメールの特徴

- ・金融機関、宅配事業者、大手ショッピングサイト、クレジットカード会社等を装ったメールやSMSが多く確認される。
- ・その他にも国税庁や警察庁、鉄道会社、ETC利用サービスを装うメール等も散見される。
- ・リンク（URL）や文字をクリックさせ偽サイトに誘導する。
- ・メール内容は、【重要】【至急】【未払い料金】【荷物の不在通知】等の言葉で利用者を急かし、リンクをクリックさせようとする。

フィッシング被害防止対策

- ◆メールやSMSのリンクを安易に開かない
- ◆IDやパスワード、カード情報を不用意に入力しない
- ◆専用アプリやブックマークから正規サイトを利用する
- ◆内容に身に覚えがなければ電話や店頭、公式サイトで直接確認する
- ◆ウイルス対策ソフトやOS、ソフトウェアをアップデートして最新の状態に保つ

メールやSMSを受信したときは慌てず、信用せず、疑いましょう



フィッシング被害防止対策動画

YouTube 福岡県警察公式チャンネル
【サイバー犯罪対策課】
<https://youtu.be/Y4cxMZMa5yQ>

